(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 923 828 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
28.01.2004 Bulletin 2004/05

(21) Application number: **97940111.4**

(22) Date of filing: **15.08.1997**

(51) Int Cl.[7]: **H04L 9/08**

(86) International application number:
PCT/EP1997/004575

(87) International publication number:
WO 1998/010560 (12.03.1998 Gazette 1998/10)

(54) QUANTUM CRYPTOGRAPHY DEVICE AND METHOD

QUANTENKRYPTOGRAPHISCHES GERÄT UND VERFAHREN

DISPOSITIF ET PROCEDE DE CRYPTOGRAPHIE QUANTIQUE

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **05.09.1996 US 25839 P**

(43) Date of publication of application:
23.06.1999 Bulletin 1999/25

(73) Proprietor: **Swisscom AG**
3000 Bern 29 (CH)

(72) Inventors:
- **GISIN, Nicolas**
  CH-1206 Genève (CH)
- **HUTTNER, Bruno**
  F-74160 Collonges-sous-Salève (FR)
- **MULLER, Antoine**
  CH-1203 Genève (CH)
- **ZBINDEN, Hugo**
  CH-1203 Genève (CH)
- **PERNY, Beat**
  CH-3213 Kleinbösingen (CH)

(74) Representative: **BOVARD AG - Patentanwälte**
Optingenstrasse 16
3000 Bern 25 (CH)

(56) References cited:
WO-A-95/07583 **US-A- 5 307 410**

EP 0 923 828 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This invention relates to an optical communication system and method configured for the distribution of a key using quantum cryptography.

Prior Art.

[0002] The purpose of cryptography is to exchange messages in perfect privacy between two users, conventionally known as Alice and Bob. Cryptography methods often use a publicly announced encrypting and decrypting algorithm; the confidentiality of the information relies entirely on a key which must be used as an input to the decrypting algorithm for decrypting the received messages.

[0003] The key usually consists of a randomly chosen, sufficiently long string of bits. Once the key is established, subsequent messages can be transmitted safely over a public channel. However, two users wanting to communicate must at a certain stage use a secure channel to share the key. With conventional key transmission methods, which can be subject to passive monitoring by an eavesdropper, it is impossible to transmit a certifiably secret key, and cumbersome physical security measures are required. However, secure key distribution is possible using quantum techniques. In quantum cryptography, the key is exchanged through a quantum channel. Its security is based on the principles of quantum mechanics which state that any measurement of a suitably chosen quantum system will inevitably modify the quantum state of this system. Therefore, an eavesdropper, Eve, might get information out of a quantum channel by performing a measurement, but the legitimate users will detect her and hence not use the key. In practice the quantum system may be a single photon propagating through an optical fiber, and the key can be encoded by its polarization or by its phase, as proposed by Ch. Bennett and G. Brassard in « Quantum Cryptography : Public key distribution and coin tossing ». *Proceedings of the International Conference on Computers, Systems and Signal Processing,* Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984).

[0004] Interferometric quantum key distribution systems are usually based on a double Mach-Zehnder interferometer, one side for Alice and one for Bob (see Fig. 1). These interferometers implement time-multiplexing, as both interfering pulses follow the same path between Alice and Bob, with some time delay. However, the pulses follow different paths within both Alice's and Bob's interferometers. In order to obtain a good interference, both users therefore need to have identical interferometers, with the same coupling ratios in each arm and the same path lengths, and also need to keep them stable within a few tens of nanometers during a transmission. Therefore, one interferometer has to be adjusted to the other every few seconds to compensate thermal drifts. Moreover, since optical components like phase modulators are polarization dependent, polarization control is necessary both in the transmission line and within each interferometer. In polarization-based systems, the polarization has to be maintained stable over tens of kilometers, in order to keep aligned the polarizers at Alice's and Bob's. Obviously, this is inconvenient for practical applications.

[0005] One technical problem the invention wishes to solve is thus to find an improved device and an improved method of quantum cryptography.

[0006] According to various aspects of the present invention, these improvements follow from the features of the characterizing part of the independent claims.

[0007] More specifically, these improvements follow from one system in which the interfering pulses run over the same branches of the interferometer, but in another sequence. so that they are delayed in time when they run over said quantum channel.

[0008] The system of the invention thus allow a system to be built which needs no alignment or balancing of the interferometer. Using the system of the invention. Alice and Bob can thus exchange information, e.g. a cryptographic key, through a standard telecommunication channel. The users at both ends of a channel only need to plug in the inventive sending/receiving station and the inventive key encoding station, synchronize their signals, and start the exchange.

[0009] According to another aspect of the present invention, cancellation of polarization effects is obtained by using Faraday mirrors at the end of the fibers.

[0010] The invention will be explained in more detail, by way of example, with reference to the drawings in which:

Figure 1 is a schematic representation of a conventional Mach-Zehnder interferometer for quantum cryptography, according to the prior art.

Figure 2 is a schematic representation of a first embodiment of a device according to the invention.

Figure 3 is a schematic representation of a second embodiment of a device according to the invention.

Figure 4 is a schematic representation of a third embodiment of a device according to the invention.

[0011] Figure 1 shows a block diagram of a conventional Mach-Zehnder interferometer for quantum cryptography, as described for instance in U.S. Patent No. 5307410 (Benett). A laser source 40 in Alice's device emits a short laser pulse toward Bob. The laser pulse is split into two time-shifted pulses P1 and P2 by Alice: one goes through a short path and through a phase-modulator 42 ; and the second is delayed by a longer path 43. Two couplers (beam-splitters) 41 and 44 are needed to split the laser pulse. Information about the key is encoded in the phase shift introduced by the phase modulator

42.

[0012] After propagation along the optical fiber 3, the two time-shifted pulses P1 and P2 arrive in a similar interferometer on Bob's side, creating three pulses. The first pulse is produced from P1 running over a short branch. comprising a phase modulator 51, on Bob's side. The last pulse is produced from P2 running over a delaying part 52 on Bob's side. Those two pulses carry no information on the phase setting. The middle pulse is obtained by interference between P1 running over the delay line on Bob's side with P2 running over the short branch 51. The relative phase settings creates a constructive or destructive interference in the detectors 55 and 56.

[0013] In order to obtain a good visibility, the two interferometers 4 and 5 have to be kept identical, and should preserve polarization. In particular, the length of the delay lines 43, 52 in both interferometers must be exactly the same. This is usually done, according to the prior art, by adjusting one interferometer to the other every few seconds to compensate thermal drifts

[0014] A first embodiment of an optical communication system configured for the distribution of a key using quantum cryptography according to the invention, implementing phase-encoded quantum key distribution, and based on time multiplexing, is shown on Figure 2. This embodiment features a 2 x 2 coupler 12. In principle, we have an unbalanced Michelson interferometer at Bob's side (1) with one long arm going to Alice. On Bob's side, the sending/receiving station 1 comprises a pulsed laser 10, a first coupler 11, a Faraday mirror 16, a second coupler 12, a phase modulator 13, a second Faraday mirror 14 and a single photon detector 17. The laser 10 may be, e.g., a DFB laser and produces e.g. 300ps long pulses at 1300 nm, with a repetition rate of e.g. 1 kHz. On Alice's side, the key encoding station 2 comprises a coupler 20, a detector 23, a phase modulator 21, a Faraday mirror 22 and an attenuator 24 controlled by the detector 23. Alice and Bob's device are coupled on both side of a quantum channel 3, for example, on both sides of an optical channel comprising a single mode optical fiber.

[0015] Bob initiates the transmission by sending a short laser pulse towards Alice. Let us for the moment disregard the effects of the Faraday mirrors 16, 14 22, and consider them as usual mirrors The need for coupler 20 and detector 23 in Alice's arm will also be expiained later. The pulse arriving in the coupler 12 is split into two parts : one part, P1, goes directly towards Alice; while the second part, P2, is first delayed by one bounce in the mirrors 14 and 16 (delay line). The two pulses, P1 and P2, travel down the fiber to Alice. In order to encode her bits, Alice lets the first pulse P1 be reflected by the mirror 22, but modulates the phase of the second pulse P2 by means of a phase modulator 21 situated in front of the mirror 22 (phase shift $\varnothing_A$.). The two pulses then travel back to Bob. Detection on Bob's side is done by delaying part of P1 in the same delay line 14-16. Bob lets pulse P2 unaltered but modulates the phase of the first pulse P1 with the phase modulator 13 situated in front of the mirror 14 (phase shift $\varnothing_B$). This pulse then interferes with P2. If the phase modulators at both Alice's and Bob's are off, or if the difference $\varnothing_A - \varnothing_B = 0$ (same phase shift applied to the two pulses P1 and P2), then the interference will be constructive (the two pulses follow exactly the same path). If however Alice or Bob change their phase setting between the two pulses, the interference may become destructive. Totally destructive interference is obtained when : $\varnothing_A - \varnothing_B = \pi$, where $\varnothing_A$ and $\varnothing_B$ are the total phase shifts introduced by Alice and Bob respectively, i.e. the phase shifts corresponding to a return trip through the phase modulators. In this case no light is detected at single photon detector 17. Note that it is essential that the interference obtained when the phase shifts are different is totally destructive. This ensures that, when Bob obtains a detection event, he can be certain that Alice did not use a different phase, and thus that she used the same phase as himself.

[0016] This shows that the relative phase setup modulates the intensity in the detector 17, and thus can be used to transfer information from Alice to Bob. The first attractive features of this setup are that the interferometer is automatically aligned (both pulses are delayed by the same delay line), and that the visibility of the fnnges is independent of the transmission/reflection coefficients of the coupler 12.

[0017] Of course, a large fraction of the light does not follow these two paths, but is split differently at various couplers (e.g. keeps oscillating a few times between 14-16 or 16-22 before leaving towards the detector 17). These pulses will eventually arrive in the detector 17, but at a different time, and will be easily discriminated. Therefore, they do not reduce the visibility. Of particular interest is the fraction of P1 coming back from Alice to Bob, and which goes directly onto the detector 17, thus arriving before the two interfering pulses. We shall show in the following that this pulse is required to prevent some type of eavesdropping strategy. Please note that, as the distance between Alice and Bob is much longer than the length of Bob's interferometer, the time delay between the two pulses arriving in Bob's setup (i.e. the time between P2 leaving and P1 coming back) is much longer than the time between the pulses in Alice's setup : a span of 10 km between Alice and Bob corresponds to 0.1 ms. This means that Bob's station needs to remain stable for times longer than that, but this is not a problem for a short interferometric system. On the other hand, assuming a distance between the mirrors 14 and 16 of 3 m, the time delay between the pulses arriving at Alice's is only 30 ns. This means that there is absolutely no problem of stability, even for a very long transmission line. However, in order to encode her bits, Alice needs to have a fast phase modulator 21 (about 100 MHz). This fast modulation is needed in order to be able to modulate tne phase of the pulse P2 arriving at Alice's, without altering the phase of P1. This is no problem with

existing Lithium Niobate ($LiNbO_3$) modulators A similar, or slower, phase modulator may be used on Bob's side. Other phase modulators are described in WO96/07951.

[0018] The above setup would work perfectly well for ideal fibers, with no birefringence. Unfortunately. all existing optical fibers have birefringence, which will modify the state of polarization of the light, and may lead to a reduction in the visibility of the interference. In order to preserve interference, we use instead of usual mirrors so-called Faraday mirrors 14, 16, 22. A Faraday mirror is simply an ordinary mirror, glued on a Faraday rotator, which rotates the polarization by 45°.

[0019] The effect of a Faraday mirror is to transform any polarization state into its orthogonal, i.e., the polarization state of the reflected pulse on each point of the optical fiber is orthogonal to the polarization state of the received pulse. Replacing ordinary mirrors 14 and 16 by Faraday mirrors (i.e., adding the Faraday rotators) thus ensures that the two pulses P1 and P2 have the same polarization, irrespective of birefringence effects in the delay line 14-16. Therefore, the polarization state of the pulse P2 is unchanged by the double bounce on the Faraday mirrors 14 and 16, and similarly for the state of P1 bouncing on the Faraday mirrors 16 and 14 on its way to the detector 17. Note that the above is not necessarily true for the pulses P1 and P2 propagating down the long transmission fiber (several kilometers long). Due to the influence of the earth magnetic field, which creates a small Faraday effect in the fiber itself, and of possible rapid fluctuations in the birefringence, the polarization state of the returning pulses is not necessarily orthogonal to the input polarization state. However, what is important in our setup is that the two interfering pulses P1 and P2 have the same polarization.

[0020] Use of a Faraday mirror 22 in Alice's enables one to compensate for the polarization dependence of the phase modulator 21, as well as for polarization dependent losses.

[0021] Until now, we have only discussed macroscopic pulses. In order to get quantum cryptographic security, the information carrying pulses need to be very weak, with at most one photon per pulse, as explained by C. H. Benett, G. Brassard and A.K Ekert, « Quantum Cryptography », *Scientific American 267,* pp. 50-57, 1992. This is to prevent a malevolent eavesdropper, known as Eve, to divert part of the pulse and get information on the key. In practice, we rely on strongly attenuated laser light. Since the photon distribution of this light is Poissonian, in order to ensure that the probability of more than one photon is weak enough, we use about 0.1 photon per pulse on average. This attenuation may be obtained by adding the extra strongly transmitting coupler 20 in Alice's arm with a transmission coefficient $t_3 \approx 1$. This creates enough attenuation on the beams reflected by the mirror 22 to have a single-photon-like pulse sent back to Bob, as well as maximizes the intensity going to the detector 23, and thus enables an ordinary detector 23 to be used, and not a single-photon one. If the attenuation is not sufficient, Alice may add an extra attenuator 24, controlled by the detector 23, in front of her setup. Using the detector 23, Alice can monitor the intensity of the incoming pulses, and control the attenuation to ensure that the pulse P2 going back to Bob has indeed the correct intensity. (Remember that the pulses going from Bob to Alice do not carry any phase information yet ; it is only on the way back to Bob that the phase chosen by Alice is encoded in the pulse P2.

[0022] Monitoring the incoming intensity has the added advantage that Alice can detect any attempt by Eve to obtain the value of her phase shift by sending much stronger pulses in the system, and measuring the phase of the reflected pulses.

[0023] On Bob's side, the light detector 17 needs to be a single-photon detector, for instance an LN_2-cooled avalanche photo diode biased beyond breakdown and operating in the Geiger mode. The bias voltage of the diode is the sum of a DC part well below threshold and a short, for instance 2ns, rectangular pulse that pushes the diode e.g. 1.0 V over threshold when a photon is expected. This time window allows the number of dark-counts to be reduced considerably and for discriminating non relevant pulses. Furthermore, in order to obtain as much of the light as possible on the detector 17, the coupler 11 has to be strongly transmitting, with transmission coefficient $t_1 \approx 1$.

[0024] This system can be used to implement B92 protocol, or two-states protocol, suggested by C.H. Bennet in « Quantum Cryptography Using Any Two Non-orthogonal States », *Physical Review Letters 68*, pp. 3121-3124, 1992. Both Alice and Bob choose at random their phase settings, so that the overall phase shifts in the phase modulators 13 and 21 are 0 or π, corresponding, respectively, to bit value 0 and 1. Note that these are overall phase shifts, corresponding to the return trip of the pulses. Therefore, if a detection, i.e. constructive interference, occurred, Alice and Bob know that they applied the same phase shift, and that they had the same bit value : if Bob chooses bit 0, and gets one count in his detector, he knows that Alice has also sent a 0, and reciprocally for bit 1.

[0025] If Alice and Bob use different phase shifts, the difference is always π, which means that the interference in the single photon detector 17 is always destructive, and that no count should be registered. Of course, since they use very weak pulses, in many instances Bob would get no count in the detector 17. In this case, he cannot infer what was sent by Alice : it could be that Alice used a different phase; or it could be that there was simply no photon in the pulse. We can now understand why very weak pulses are needed : if Alice and Bob use strong pulses, which always carry more than one photon, Bob would always know the bit sent by Alice : one count, same choice of phase; no count, different choice of phase. Unfortunately, so would Eve. For example, she could simply split the pulses, by adding an extra

coupler on the line, and by measuring the phase of the pulses sent by Alice. However, if the pulse sent by Alice possesses at most one photon, this simple eavesdropping strategy fails completely : if Eve measures the photon, then Bob will not get it, and would simply discard the corresponding transmission.

[0026] Another eavesdropping strategy on two-state systems would be for Eve to stop the transmission altogether, measure as many pulses as she could, and send to Bob only the ones she managed to obtain. To prevent this, Alice needs to send both a strong pulse P1, as a reference, and a weak one P2, containing the phase information. Eve cannot suppress the strong pulse without being immediately discovered. If she suppresses only the weak one, because she did not obtain the phase information, the strong pulse alone will introduce noise in the detector 17. In the system of the invention, this is easily implemented by using a strongly asymmetric coupler 12, with transmission coefficient $t_2 \approx 1$, and reflection coefficient $r_2 \approx 0$. In this case, the pulse P1 going back towards Bob is much stronger than the pulse P2, which has already been through the 14-16 delay line, and thus was strongly attenuated. Bob can detect the part of the pulse P1 going directly to the detector 17, before looking at the interference. It is also possible to add an extra coupler and detector in front of the Faraday mirror 16, in a way similar to Alice's setup.

[0027] The same setup, but with different choices of phase for Alice and Bob can be used to implement other protocols, such as the BB84 protocol described by Ch. Bennett and G. Brassard in « Quantum Cryptography : Public key distribution and coin tossing », *Proceedings of the International Conference on Computers, Systems and Signal Processing,* Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). According to this protocol, Alice chooses among four possible states. In another example, if Alice's phase shifts are not 0 and $\pi/2$, but 0 and any angle α, it is easy for Bob to compensate by using $\pi - \alpha$ and n, so that when Bob uses the wrong phase shift, the interference is totally destructive.

[0028] Figure 3 shows a block diagram of a second embodiment of an optical communication system according to the invention, configured for the distribution of a key using quantum cryptography and implementing phase-encoded quantum key distribution. This embodiment features a 3 x 3 coupler 12'. On Alice's side, the same key encoding station 2 as in the first embodiment can be used. On Bob's side, the sending/receiving station 1 comprises a laser 10, a 3x3 coupler 12', a first Faraday mirror 14, a second Faraday mirror 16, and two single-photon detectors 17 and 18.

[0029] The first pulse P1 follows the following sequence of branches :

Laser 10 - mirror 16 - mirror 22 (on Alice's) - mirror 16 (on Bob's)-mirror 14 - detectors 17, 18.

[0030] The other pulse P2 follows the following sequence of branches :

Laser 10 - mirror 16 - mirror 14 - mirror 16 -mirror 22 (on Alice's) and to the detectors 17, 18.

[0031] Depending on the phase difference between the pulses P1 and P2, a constructive interference will be detected either on the detector 17 or on the detector 18. The choice of phase by Alice, either $\pi/3$ or $-\pi/3$ sends the photon either in the detector 17 or in the detector 18 respectively.

[0032] The main advantage of using two detectors 17 and 18 is that we do not need a second phase modulator on Bob's side to implement the B92 protocol. The drawback is the need for two single photon detectors 17 and 18.

[0033] Adding a second phase modulator before the Faraday mirror 14, as in the previous system, enables the BB84 system to be efficiently implemented: Alice chooses among the four possible phases : $\pi/3$, $-\pi/3$, $2\pi/3$ and $-2\pi/3$; while Bob chooses only between 0 (which enables him to differentiate between $\pi/3$ and $-\pi/3$), and π (which enables him to differentiate between $2\pi/3$ and $-2\pi/3$).

[0034] Figure 4 shows a block diagram of a third embodiment of an optical communication system according to the invention, configured for the distribution of a key using quantum cryptography and implementing polarization-encoded quantum key distribution. This embodiment features a polarization coupler 12" on Bob's side.

[0035] On Alice's side, the same key encoding station 2 as in the first embodiment can be used. On Bob's side, the sending/receiving station 1 comprises a laser 10, a polarization controller 100, a first coupler 11, a polarization coupler 12", a first Faraday mirror 14, a second Faraday mirror 16, and a single-photon polarization detection system 17'. Again, no phase modulator is needed on Bob's side.

[0036] The laser 10 uses a polarization controller 100 to send the light with e.g. right circular polarization. The polarization coupler 12" separates the vertical and horizontal polarizations. One of the polarization components, say the vertical one, follows the following sequence of branches (with a polarization switch from vertical to horizontal, and vice versa, each time it is reflected by one of the Faraday mirrors) :

Laser 10 - mirror 22 (on Alice's) - mirror 16 (on Bob's) - mirror 14-polarization detection system 17'.

[0037] On the other hand. the other polarization component (the horizontal one) follows the sequence :

Laser 10 - mirror 14 - mirror 16 - mirror 22 (on Alice's) and to the detection system 17'.

[0038] When the two orthogonally polarized pulses

recombine at the polarization coupler 12', the polarization of the outgoing pulse depends on their relative phase. For example. a zero phase shift corresponds to right circular polarization (identical to the initial one). while a π phase shift corresponds to left circular polarization, and $\pm\pi/2$ phase shifts give linear polarization at = 45° A phase change in the phase modulator 21 thus corresponds to a different output polarization. This embodiment thus does not require a second phase modulator on Bob's side, even for the BB84 protocol. Moreover, by using four different choices of phase in the phase modulator 21, four different states can be encoded. The drawback of this embodiment is that it requires a more complicated detection system 17' which can separate the various polarizations. Furthermore, it does require the polarization of the returning pulses to be orthogonal to the polarization of the incoming ones. Therefore, fast polarization fluctuations and the influence of the earth magnetic field may limit the length of the transmission line 3.

[0039] Even good single-photon detectors makes errors and occasionally miss photons or count one photon when no photon is actually received (darkcounts). Error correction means, for instance using cyclic redundancy checks, may therefore be provided in Bob's.

[0040] Even if the sending/receiving station 1 and the key communicating station 2 are shown as two separates devices in the above specification, it can also be useful to combine a sending/receiving station and a key communicating station in the same device. This combined device can then alternatively play the role of Bob or of Alice, i.e. initiate a key transmission or answer to another device and transmit a key.

[0041] Any embodiment of the system of the invention can be easily extended to a multi-stations system, i.e. to a system for distributing a key simultaneously to several mutually connected stations, as suggested for instance in WO95/07583.

[0042] The embodiment of figure 4 is particularly advantageous from this point of view, as less delayed pulses are sent over the quantum channel.

Claims

1. Method of communicating between two stations (1, 2) using an interferometric system for quantum cryptography, comprising the step of sending at least two light pulses over a quantum channel (3) and detecting the interference created by said pulses in one station, **characterized in that** said interfering pulses run over the same branches of said interferometer, but in another sequence, so that they are delayed when they run over said quantum channel.

2. Method according to the preceding claim, **characterized in that** said pulses are reflected by at least one Faraday mirror at at least one end of said quantum channel.

3. Method according to one of the preceding claims, **characterized in that** the average number of photons in the interfering pulses is less than 1.

4. Method according to one of the preceding claims, **characterized in that** said delayed pulses are sent by a source (10) in a sending/receiving station (1) which delays the second pulses with a delay line (14-16), and received by at least one key encoding station (2) which phase modulates the second pulse and reflects both pulses toward said sending/receiving station (1) which delays and phase modulates said first pulse.

5. Method according to the preceding claim, **characterized in that** said second pulse is attenuated in said key encoding station (2) so that the average number of photons in said second pulse reflected back to said sending/receiving station (1) is less than 1.

6. Method according to one of the claims 4 or 5, **characterized in that** both stations (1, 2) choose at random the phase shift applied to said first and second pulses.

7. Method according to the preceding claim, **characterized in that** said phase shifts are chosen as either the value 0 or the value π, and **in that** the interference between said first pulse and said second pulse is constructive when both stations have applied the same phase shift, and totally destructive when they apply different phase shifts.

8. Method according to one of the claims 1 to 5, **characterized in that** the light sent comprises at least two orthogonal polarization components, and **in that** said components run over the same branches of said interferometer, but in another sequence.

9. Method according to the preceding claim, **characterized in that** one of said stations (2) chooses at random the phase of one of the above polarization components with respect to the second one, thus creating a random output polarization.

10. Interferometric system configured for the distribution of a key over a quantum channel (3) using quantum cryptography, comprising :

    at least one sending/receiving station (1) and at least one key encoding station, both connected to said quantum channel (3),

    means (10, 12, 14, 16) in at least one of said

stations (1) for sending at least two pulses over said quantum channel (3) to at least one other said station,

detectors (17 ; 17, 18 ; 17') in at least one of said stations (1) for detecting the interference created by said pulses in said station,

characterized in that said interfering pulses run over the same branches of said interferometer, but in another sequence, so that they are delayed when they run over said quantum channel.

11. System according to the preceding claim, **characterized in that** at least one of said stations (1, 2) comprises at least one Faraday mirror at at least one end of said quantum channel.

12. System according to one of the claims 10 or 11, **characterized in that** at least one of said stations (1, 2) comprises means (20, 24, 12) for attenuating the intensity of said light pulses so that the average number of photons in the interfering pulses is less than 1.

13. System according to one of the claims 10 to 12, **characterized in that** it comprises at least one sending/receiving station (1) and at least one key encoding station (2),

said sending/receiving station (1) comprising a delay line (12, 14, 16) for delaying said first pulse before it is sent over said quantum channel (3) and said second pulse received over said quantum channel (3), and at least one single photon detector (17 ; 17-18 ; 17') for detecting interferences between said first and second pulses,

said key encoding station (2) comprising mirrors (22) for reflecting said first and second pulses and at least one phase modulator (21) for modulating the phase of at least one of said pulses.

14. System according to one of the claims 10 to 13, **characterized in that** said key encoding station (2) comprises means (20 ; 24) for attenuating the intensity of at least one of said pulses so that the average number of photons in said second pulse reflected back to said sending/receiving station (1) is less than 1.

15. System according to one of the claims 10 to 14, **characterized in that** both stations (1, 2) choose at random the phase shift applied to said first and second pulses.

16. System according to one of the claims 10 to 15, **characterized in that** both stations choose said phase shifts as either the value 0 or the value π, and **in that** the interference between said first pulse and said second pulse is constructive when both stations have applied the same phase shift, and totally destructive when the stations have applied different phase shifts.

17. System according to one of the claims 10 to 14, **characterized in that** the light sent by said sending/receiving station (1) comprises at least two orthogonal components, and **in that** said components run over the same branches of said interferometer, but in another sequence.

18. System according to the preceding claim, **characterized in that** one of said stations (2) chooses at random the phase of one of the above polarization components with respect to the second one, thus creating a random output polarization.

19. Key encoding station (2) for communicating a key to at least one sending/receiving station (1) through a quantum channel (3), **characterized by** :

- reflecting means (22) for reflecting a first pulse sent by a receiving station (1) back to said receiving station (1),
- reflecting means (22) for reflecting a second pulse, sent by said receiving station (1) shortly after said first pulse, back to said receiving station (1).
- modulating means (21) for modulating the phase of said second pulse with respect to said first pulse.

20. Key encoding station according to the preceding claim, **characterized by** detecting means (23) for detecting said first pulse.

21. Key encoding station according to the preceding claim, **characterized in that** said first pulse and said second pulse both run through said modulating means (21) and are both reflected by the same reflecting means (22), and **in that** said detecting means (23) adjust the phase shift applied by said modulating means (21) immediately after having received said first pulse, so that only said second pulse is phase modulated by said phase modulating means (21).

22. Key encoding station according to the preceding claim, **characterized in that** it chooses at random the phase shift applied to said second pulse.

23. Key encoding station according to the preceding claim, **characterized in that** the phase shift applied by said modulating means is chosen at random among as either the value 0 or the value π.

24. Key encoding station according to one of the claims 19 to 23, **characterized in that** it further comprises an attenuating means (20, 24) for attenuating the light intensity of said second pulse so that the average number of photons in said second pulse reflected back is less than 1.

25. Key encoding station according to claim 24, **characterized in that** said attenuating means comprises a coupler (20) sending most of the received light to said detecting means (23).

26. Key encoding station according to claim 24 or 25, **characterized in that** said attenuating means comprise an attenuator controlled by said detecting means.

27. Key encoding station according to one of the claims 19 to 26, **characterized in that** said reflecting means (22) are composed of a Faraday mirror.

28. Key encoding station according to one of the claims 20 to 27, **characterized in that** said detecting means are not single-photon detectors.

29. Key encoding station according to one of the claims 19 to 28, **characterized in that** said modulating means (21) are made of a Lithium Niobate ($LiNbO_3$) modulator.

30. Sending/receiving station (1) for receiving a key sent from one key encoding station (2) through a quantum channel (3), **characterized by** :

a pulsed laser source (10),

a delay line (14, 16),

detecting means (17, 18, 17')

a first coupler (12) connected in such a way that the pulses emitted by said pulsed laser source are split in two pulses, wherein the first split pulse is directly sent to said quantum channel whereas the second split pulse is delayed by said delay line (14, 16) before being sent to said quantum channel, and that the pulses received from said quantum channel (3) are split in two pulses, wherein the first pulse is directly sent to said detecting means (17, 18, 17') whereas the second pulse is delayed by said delay line (14, 16) before being sent to said detecting means (17, 18, 17').

31. Sending/receiving station according to the preceding claim, **characterized by** modulating means (13) for modulating the phase of the received pulses delayed by said delay line (14, 16).

32. Sending/receiving station according to the preceding claim, **characterized in that** said modulating means (13) choose at random the phase shift applied to said delayed pulses.

33. Sending/receiving station according to the preceding claim, **characterized in that** said modulating means (13) choose said phase shifts at random as either the value 0 or the value π.

34. Sending/receiving station according to one of the claims 31 to 33, **characterized in that** said modulating means (21) are made of a Lithium Niobate ($LiNbO_3$) modulator.

35. Sending/receiving station according to claim 30, **characterized in that** it comprises two detectors (17, 18), **in that** said first coupler (12') is a 3x3 coupler connected to said detectors (17, 18), and **in that** a pulse will be sent either on the first (17) or on the second (18) of said detectors depending on the interference created in said coupler (12').

36. Sending/receiving station according to claim 30, **characterized in that** said laser source (10) sends light pulses with a circular polarization, and **in that** said first coupler (12") is a polarization coupler that separates the vertical and horizontal polarizations of the pulses.

37. Sending/receiving station according to one of the claims 30 to 36, **characterized in that** said delay line (14, 16) comprises two Faraday mirrors (14, 16) reflecting the delayed pulses.

38. Sending/receiving station according to one of the claims 30 to 37, **characterized in that** said detecting means (17, 18, 17') are single-photon detectors.

39. Sending/receiving station according to the preceding claim, **characterized in that** said single-photon detectors (17, 18, 17') are avalanche photo diodes biased beyond reverse breakdown and operating in the Geiger mode.

40. Sending/receiving station according to one of the claims 38 or 39, **characterized in that** in order to reduce the number of darkcounts the single-photon detectors are activated only each time a photon is expected.

41. Sending/receiving station according to one of the claims 30 to 40, **characterized in that** said pulsed laser source is a DFB laser.

42. Sending/receiving station according to one of the claims 30 to 41, further comprising error correcting means.

43. Device for the distribution of a key over a quantum channel (3) using quantum cryptography, **characterized in**

that it comprises a sending/receiving station (1) for receiving a key sent from one key encoding station (2) through a quantum channel (3), whereas the sending/receiving station (1) comprises a pulsed laser source (10), a delay line (14, 16), detecting means (17, 18, 17') and a first coupler (12) connected in such a way that the pulses emitted by said pulsed laser source are split in two pulses, wherein the first split pulse is directly sent to said quantum channel whereas the second split pulse is delayed by said delay line (14, 16) before being sent to said quantum channel, and that the pulses received from said quantum channel (3) are split in two pulses, wherein the first pulse is directly sent to said detecting means (17, 18, 17') whereas the second pulse is delayed by said delay line (14, 16) before being sent to said detecting means (17, 18, 17'), and

that it comprises a key encoding station (2) for communicating a key to at least one sending/receiving station (1) through a quantum channel (3), whereas the sending/receiving station (1) comprises reflecting means (22) for reflecting a first pulse sent by a receiving station (1) back to said receiving station (1), reflecting means (22) for reflecting a second pulse, sent by said receiving station (1) shortly after said first pulse, back to said receiving station (1) and modulating means (21) for modulating the phase of said second pulse with respect to said first pulse.

44. Multi-stations system for the distribution of a key over a quantum channel (3) using quantum cryptography between at least one sending/receiving station (1) and at least one key encoding station (2), **characterized in**

that it comprises a sending/receiving station (1) for receiving a key sent from one key encoding station (2) through a quantum channel (3), whereas the sending/receiving station (1) comprises a pulsed laser source (10), a delay line (14, 16), detecting means (17, 18, 17') and a first coupler (12) connected in such a way that the pulses emitted by said pulsed laser source are split in two pulses, wherein the first split pulse is directly sent to said quantum channel whereas the second split pulse is delayed by said delay line (14, 16) before being sent to said quantum channel, and that the pulses received from said quantum channel (3) are split in two pulses, wherein the first pulse is directly sent to said detecting means (17, 18, 17') whereas the second pulse is delayed by said delay line (14, 16) before being sent to said detecting means (17, 18, 17'), and

that it comprises a key encoding station (2) for communicating a key to at least one sending/receiving station (1) through a quantum channel (3), whereas the sending/receiving station (1) comprises reflecting means (22) for reflecting a first pulse sent by a receiving station (1) back to said receiving station (1), reflecting means (22) for reflecting a second pulse, sent by said receiving station (1) shortly after said first pulse, back to said receiving station (1) and modulating means (21) for modulating the phase of said second pulse with respect to said first pulse.

Patentansprüche

1. Kommunikationsverfahren zwischen zwei Vorrichtungen (1, 2) mittels eines interferometrischen Systems zur Quantenkryptographie, wobei mindestens zwei Lichtpulse über einen Quantenkanal (3) geschickt werden und in einer Vorrichtung die durch die genannten Pulse verursachte Interferenz detektiert wird, **dadurch gekennzeichnet, dass** die genannten interferierenden Pulse über dieselben Zweige des genannten Interferometers übertragen werden, jedoch in einer anderen Sequenz, so dass sie verzögert über den genannten Quantenkanal übertragen werden.

2. Verfahren nach Anspruch 1 **dadurch gekennzeichnet, dass** die genannten Impulse durch mindestens einen Faraday-Spiegel bei mindestens einem Ende des genannten Quantenkanals reflektiert werden.

3. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, dass** die mittlere Anzahl von Photonen in den interferierenden Pulsen kleiner als 1 ist.

4. Verfahren nach einem der Ansprüche 1 bis 3 **dadurch gekennzeichnet, dass** die genannten verzögernden Pulse durch eine Quelle (10) in einer Sende/Empfangsvorrichtung (1) gesendet werden, welche den zweiten Impuls mit einer Verzögerungslinie (14 - 16) verzögert, und dass die genannten verzögernden Pulse durch mindestens eine Entschlüsselungsvorrichtung (2) empfangen werden, die den zweiten Puls phasenmoduliert und beide Pulse zur genannten Sende/Empfangsvorrichtung (1) reflektiert, was den genannten ersten Puls verzögert phasenmoduliert.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet dass** der genannte zweite Puls in der genannten Verschlüsselungsvorrichtung (2) abgeschwächt wird, so dass die mittlere Anzahl Photonen kleiner als 1 ist, die im genannten zweiten Puls zurück zur genannten Sende/Emp-

fangsstation (1) reflektiert werden.

6. Verfahren nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet, dass** die beiden Vorrichtungen (1, 2) zufällig den Phasenshift wählen, welcher an die genannten ersten und zweiten Pulse angelegt wird.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die genannten Phasenshifts entweder mit dem Wert 0 oder mit dem Wert π gewählt werden und dass die Interferenz zwischen dem genannten ersten Puls und dem genannten zweiten Puls konstruktiv ist, wenn beide Vorrichtungen den gleichen Phasenshift anwenden, und vollständig destruktiv ist, wenn sie unterschiedliche Phasenshifts anwenden.

8. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** das gesendete Licht mindestens zwei orthogonal polarisierte Komponenten umfasst und dass die genannten Komponenten sich über die gleichen Zweige des genannten Interferometers bewegen, jedoch in einer anderen Sequenz.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** eine der genannten Vorrichtungen (2) zufällig die Phase einer der genannten polarisierten Komponenten in Bezug auf die zweite wählt, wodurch eine zufällige Ausgangspolarisation gewählt wird.

10. Interferometrisches System, das zur Verteilung eines Schlüssels über einen Quantenkanal (3) zur Verwendung bei Quanten Kryptographie konfiguriert ist, welches umfasst:

    mindestens eine Sende/Empfangsvorrichtung (1) und mindestens eine Verschlüsselungsvorrichtung, die beide mit dem genannten Quantenkanal (3) verbunden sind,

    Mittel (10, 12, 14, 16) in mindestens einer der genannten Vorrichtungen (1) zum Senden von mindestens zwei Pulsen über den genannten Quantenkanal (3) zu mindestens einer der genannten Vorrichtungen,

    Detektoren (17; 17, 18; 17') in mindestens einer der genannten Vorrichtungen (1) zum Detektieren der Interferenz, die durch die genannten Pulse in der genannten Vorrichtung erzeugt werden,

    dadurch gekennzeichnet, dass die genannten interferierenden Pulse über dieselben Zweige des genannten Interferometers gehen, jedoch in einer anderen Sequenz, so dass sie verzögert sind, wenn sie über den genannten Quantenkanal gehen.

11. System nach Anspruch 10, **dadurch gekennzeichnet, dass** mindestens eine der genannten Vorrichtungen (1, 2) mindestens einen Faraday-Spiegel an mindestens einem Ende des genannten Quantenkanals umfasst.

12. System nach einem der Ansprüche 10 oder 11, **dadurch gekennzeichnet, dass** mindestens eine der genannten Vorrichtungen (1, 2) Mittel (20, 24, 12) zum Abschwächen der Intensität des genannten Lichtpulses umfasst, so dass die mittlere Anzahl Photonen in den interferierenden Pulsen kleiner als 1 ist.

13. System nach einem der Ansprüche 10 bis 12, **dadurch gekennzeichnet, dass** es mindestens eine Sende/Empfangsvorrichtung (1) und mindestens eine Entschlüsselungsvorrichtung (2) umfasst,

    wobei die genannte Empfangsvorrichtung (1) eine Verzögerungslinie (12, 14, 16) zum Verzögern des genannten ersten Pulses umfasst, bevor dieser über den genannten Quantenkanal (3) geschickt wird und der genannte zweite Puls über den genannten Quantenkanal (3) empfangen wird, und wobei die genannte Sende/Empfangsvorrichtung (1) mindestens einen Einzelphotonendetektor (17; 17 - 18; 17') zum Detektieren von Interferenzen zwischen den genannten ersten und zweiten Pulsen umfasst,

    wobei die genannte Verschlüsselungsstation (2) Spiegel (22) zum Reflektieren der genannten ersten und zweiten Pulse und mindestens einen Phasenmodulator (21) zum Modulieren der Phase von mindestens einem der genannten Pulse umfasst.

14. System nach einem der Ansprüche 10 bis 13, **dadurch gekennzeichnet dass** die genannte Verschlüsselungsvorrichtung (2) Mittel (20; 24;) zum Abschwächen der Intensität von mindestens einem der genannten Pulse umfasst; so dass die mittlere Anzahl Photonen in dem genannten zweiten Puls, der zu der genannten Sende/Empfangsvorrichtung (1) reflektiert wird, kleiner als 1 ist.

15. System nach einem der Ansprüche 10 bis 14, **dadurch gekennzeichnet, dass** beide Vorrichtungen (1, 2) die an die ersten und zweiten Pulse angelegten Phasenshifts zufällig wählen.

16. System nach einem der Ansprüche 10 bis 15, **dadurch gekennzeichnet, dass** beide Vorrichtungen die genannten Phasenshifts entweder mit dem Wert 0 oder mit dem Wert π anwenden und dass die Interferenz zwischen dem genannten ersten und

zweiten Puls konstruktiv ist wenn beide Vorrichtungen den gleichen Phasenshift anwenden und vollständig destruktiv wenn die Vorrichtung unterschiedliche Phasenshifts anwenden.

17. System nach einem der Ansprüche 10 bis 14 **dadurch gekennzeichnet, dass** das Licht, das durch die genannte Sende/Empfangsvorrichtung (1) geschickt wird, mindestens orthogonale Komponenten umfasst, und dass die genannten Komponenten über den gleichen Zweig des genannten Interferometers gehen, jedoch in einer anderen Sequenz.

18. System nach Anspruch 17, **dadurch gekennzeichnet dass** eine der genannten Vorrichtungen (2) zufällig die Phase der oben genannten Polarisationskomponenten im Bezug auf die zweite wählt, wodurch eine zufällige Ausgangspolarisation kreiert wird.

19. Entschlüsselungsvorrichtung (2) zum Übertragen eines Schlüssels zu mindestens einer Sende/Empfangsvorrichtung (1) durch einen Quantenkanal (3), **dadurch gekennzeichnet,**

dass die Vorrichtung Reflektionsmittel (22) zum Reflektieren eines ersten Pulses umfasst, welcher Puls durch eine Empfangsvorrichtung (1) zurück zur genannten Empfangsvorrichtung (1) geschickt wird,

dass die Entschlüsselungsvorrichtung (2) Reflektionsmittel (22) zum Reflektieren eines zweiten Pulses umfasst, welcher Puls durch die genannte Empfangsvorrichtung (1) kurz nach dem genannten ersten Puls zurück zur genannten Empfangsvorrichtung (1) geschickt wird,

dass die Verschlüsselungsvorrichtung (2) Modulationsmittel (21) zum Modulieren der Phase des genannten zweiten Pulses in Bezug auf den genannten ersten Puls umfasst.

20. Entschlüsslungsvorrichtung nach Anspruch 19 **dadurch gekennzeichnet, dass** die Entschlüsslungsvorrichtung Dedektionsmittet (23) zum Detektieren des genannten ersten Pulses umfasst.

21. Entschlüsslungsvorrichtung nach Anspruch 20, **dadurch gekennzeichnet, dass** der genannte erste Puls und der genannte zweite Puls beide durch die genannten Modulationsmittel (21) gehen und beide durch die gleichen Reflektionsmittel (22) reflektiert werden und dass die genannten Detektionsmittel (23) den Phasenshift abgleichen, welchen Phasenshift durch die genannten Modulationsmittel (21) unmittelbar nach dem Empfang des ersten Pulses angelegt wird, so dass nur der genannte zweite Puls durch die genannten Phasenmodulationsmittel (21) moduliert wird.

22. Entschlüsslungsvorrichtung nach Anspruch 21, **dadurch gekennzeichnet, dass** die Entschlüsslungsvorrichtung zufällig den an den genannten zweiten Puls angelegten Phasenshift wählt.

23. Entschlüsslungsvorrichtung nach Anspruch 22, **dadurch gekennzeichnet, dass** der durch die genannten Modulationsmittel angelegte Phasenshift zufällig entweder als Wert 0 oder als Wert π gewählt wird.

24. Verschlüsslungsvorrichtung nach einem der Ansprüche 19 bis 23 **dadurch gekennzeichnet, dass** die Verschlüsslungsvorrichtung weiter Abschwächungsmittlel (20, 24) zum Abschwächen der Lichtintensität des genannten zweiten Pulses umfasst, so dass die mittlere Anzahl zurückreflektierten Photonen im genannten zweiten Puls kleiner als 1 ist.

25. Verschlüsslungsvorrichtung nach Anspruch 24, **dadurch gekennzeichnet, dass** die genannten Abschwächungsmittel einen Kuppler (20) umfassen, welcher Kuppler das meiste des empfangenen Lichts zu den genannten Detektionsmitteln (23) sendet.

26. Verschlüsslungsvorrichtung nach einem der Ansprüche 24 oder 25, **dadurch gekennzeichnet, dass** die genannten Abschwächungsmittel einen Abschwächer umfassen, der durch die genannten Detektionsmittel gesteuert wird.

27. Verschlüsslungsvorrichtung nach einem der Ansprüche 19 bis 26, **dadurch gekennzeichnet, dass** die genannten Reflektionsmittel (22) aus einem Faraday-Spiegel zusammengesetzt sind.

28. Entschlüsslungsvorrichtung nach einem der Ansprüche 20 bis 27, **dadurch gekennzeichnet, dass** die genannten Detektionsmittel nicht Einzel-Photondetektoren sind.

29. Entschlüsslungsvorrichtung nach einem der Ansprüche 19 bis 28, **dadurch gekennzeichnet, dass** die genannten Modulationsmittel (21) aus einem Lithium Niobate ($LiNbO_3$)-Modulator gemacht sind.

30. Sende/Empfangsvorrichtung (1) zum Empfangen eines Schlüssels, der von einer Verschlüsslungsvorrichtung (2) über einen Quantenkanal (3) gesendet wird, **dadurch gekennzeichnet,**

dass die Sende/Empfangsvorrichtung (1) eine gepulste Laserquelle (10) umfasst,

dass die Sende/Empfangsvorrichtung (1) eine Verzögerungslinie (14, 16) umfasst,

dass die Sende/Empfangsvorrichtung (1) Detektionsmittel (17, 18, 17') umfasst,

dass die Sende/Empfangsvorrichtung (1) einen ersten Kuppler (12) umfasst, wobei der erste Kuppler (12) derart verbunden ist, dass die durch die genannte gepulste Laserquelle emittierten Pulse in zwei Pulse geteilt werden, welcher erste geteilte Puls direkt zum genannten Quantenkanal geschickt wird und der zweite geteilte Puls durch die genannte Verzögerungslinie (14, 16) verzögert wird, bevor er zum genannten Quantenkanal geschickt wird, und dass die vom genannten Quantenkanal (3) empfangenen Impulse in zwei Pulse unterteilt werden, wobei der erste Puls direkt zu den genannten Detektionsmitteln (17, 18, 17') geschickt wird und der zweite Puls durch die genannte Verzögerungslinie (14, 16) verzögert wird, bevor er zu den genannten Detektionsmitteln (17,18,17') geschickt wird.

31. Sende/Empfangsvorrichtung nach Anspruch 30, **dadurch gekennzeichnet, dass** die Sende/Empfangsvorrichtung Modulationsmittel (13) zum Modulieren der Phase der empfangenen Pulse umfasst, die durch die genannte Verzögerungslinie (14,16) verzögert sind.

32. Sende/Empfangsvorrichtung nach Anspruch 31, **dadurch gekennzeichnet, dass** die genannten Modulationsmittel (13) zufällig den an die genannten Verzögerungsimpulse angefügten Phasenshift wählen.

33. Sende/Empfangsvorrichtung nach Anspruch 32, **dadurch gekennzeichnet, dass** die genannten Modulationsmittel (13) die genannten Phasenshifts zufällig entweder mit dem Wert 0 oder dem Wert π wählen.

34. Sende/Empfangsvorrichtung nach einem der Ansprüche 31 bis 33, **dadurch gekennzeichnet dass** die genannten Modulationsmittel (21) aus einem Lithium Niobaten ($LiNbO_3$)-Modulator gemacht sind.

35. Sende/Empfangsvorrichtung nach Anspruch 30 **dadurch gekennzeichnet, dass** die Sende/Empfangsvorrichtung zwei Detektoren (17, 18) umfasst, wobei der genannte erste Kuppler (12') ein 3x3 Kuppler ist und mit den genannten Detektoren (17,18) verbunden ist und wobei ein Puls entweder über den ersten (17) angeschlossen oder den zweiten (18) der genannten Detektoren gesendet wird, in Abhängigkeit der verursachten Interferenz in den genannten Kuppler (12').

36. Sende/Empfangsvorrichtung nach Anspruch 30, **dadurch gekennzeichnet, dass** die genannte Laserquelle (10) Lichtpulse mit einer Zirkularpolarisation sendet und dass der genannte erste Kuppler (12') ein Polarisationskuppler ist, der die vertikalen und horizontalen Polarisationen der Pulse separiert.

37. Sende/Empfangsvorrichtung nach einem der Ansprüche 30 bis 36, **dadurch gekennzeichnet, dass** die genannte Verzögerungslinie (14, 16) zwei Faraday-Spiegel (14, 16) umfasst, die die verzögerten Pulse reflektieren.

38. Sende/Empfangsvorrichtung nach einem der Ansprüche 30 bis 37, **dadurch gekennzeichnet, dass** die genannten Detektionsmittel (17, 18, 17') Einzel-Photonendetektoren sind.

39. Sende/Empfangsvorrichtung nach Anspruch 38, **dadurch gekennzeichnet, dass** die genannten Einzel-Photonendetektoren (17, 18, 17') Lawinenphotodioden sind, die über den Revers Brakedown verschoben sind und im Geiger-Modus betrieben werden.

40. Sende/Empfangsvorrichtung nach einem der Ansprüche 38 oder 39, **dadurch gekennzeichnet, dass** die Einzel-Photonendetektoren nur dann aktiviert werden, wenn ein Photon erwartet wird, um die Anzahl der Darkcounts zu reduzieren.

41. Sende/Empfangsvorrichtung nach einem der Ansprüche 30 oder 40, **dadurch gekennzeichnet, dass** die genannte gepulste Laserquelle ein DFB-Laser ist.

42. Sende/Empfangsvorrichtung nach einem der Ansprüche 30 oder 41, **dadurch gekennzeichnet, dass** die Sende/Empfangsvorrichtung weiter Fehlerkorrekturmittel umfasst.

43. Vorrichtung zum Verteilen eines Schlüssels über einem Quantenkanal (3) unter Benutzung von Quantenkryptographie, **dadurch gekennzeichnet, dass** die Vorrichtung eine Sende/Empfangsvorrichtung (1) zum Empfangen eines Schlüssels umfasst, der von einer Verschlüsslungsvorrichtung (2) durch einen Quantenkanal (3) geschickt wird, wobei die Sende/Empfangsvorrichtung (1) eine gepulste Laserquelle (10), eine Verzögerungslinie (14,17), Detektionsmittel (17,18,17') und einen ersten Kuppler (12) umfasst, welcher Kuppler derart verbunden ist, dass die durch die genannte gepulste Laserquelle emittierten Pulse in zwei Pulse gesplittet werden, wobei der erst gesplittete Puls direkt zum genannten Quantenkanal gesendet wird und der zweite gesplittete Puls durch die genannte Verzögerungslinie (14,16) verzögert wird, bevor er zum genannten Quantenkanal geschickt wird, und dass die vom genannten Quantenkanal (3) empfangenen Puls in zwei Pulse geteilt werden, wobei der erste Puls direkt zu den genannten Detektionsmitteln (17, 18,

17') geschickt wird und der zweite Puls durch die genannte Verzögerungslinie (14, 16) verzögert wird, bevor er zu den genannten Detektionsmitteln (17, 18, 17') geschickt wird, und

dass die Vorrichtung eine Verschlüsslungsvorrichtung (2) zum Übertragen eines Schlüssels zu mindestens einer Sende/Empfangsvorrichtung (1) durch einen Quantenkanal (3) umfasst, wobei die Sende/Empfangsvorrichtung (1) Reflektionsmittel (22) zum Reflektieren eines ersten Pulses umfasst, welcher erste Impuls durch eine Empfangsvorrichtung (1) zur genannten Empfangsvorrichtung (1) zurückgeschickt wird, und wobei die Sende/Empfangsvorrichtung (1) Reflektionsmittel (22) zum Reflektieren eines zweiten Pulses umfasst, welcher zweite Puls durch die genannte Empfangsvorrichtung (1) kurz nach dem genannten ersten Puls zur genannten Empfangsvorrichtung (1) und zu Modulationsmittel (21) zum Modulieren der Phase des genannten zweiten Pulses in Bezug auf den genannten ersten Puls zurückgeschickt wird.

44. Mehrstationssystem zum Verteilen eines Schlüssels über einen Quantenkanal (3) unter Benutzung von Quantenkryptographie zwischen mindesten einer Sende/Empfangsvorrichtung (1) und mindestens einer Verschlüsslungsvorrichtung (2), **dadurch gekennzeichnet,**

dass das Mehrstationssystem eine Sende/Empfangsvorrichtung (1) zum Empfangen eines Schlüssels umfasst, der über eine Entschlüsslungsvorrichtung (2) durch einen Quantenkanal (3) geschickt wird, wobei die genannte Sende/Empfangsvorrichtung (1) eine gepulste Laserquelle (10), eine Verzögerungslinie (14, 16), Detektionsmittel (17, 18, 17') und einen ersten Kuppler (12) umfasst, welcher Kuppler (12) derart verbunden ist, dass die durch die genannte gepulste Laserquelle emittierten Pulse in zwei Pulse gesplittet werden, wobei der erste gesplittete Puls direkt zum genannten Quantenkanal geschickt wird und der zweite gesplittete Puls durch die genannte Verzögerungslinie (14, 16) verzögert wird, bevor er zum genannten Quantenkanal geschickt wird und dass die vom genannten Quantenkanal (3) empfangenen Pulse in zwei Pulse gesplittet werden, wobei der erste Puls direkt zu den genannten Detektionsmitteln (17, 18, 17') geschickt wird und der zweite Puls durch die genannte Verzögerungslinie (14, 16) verzögert wird, bevor er zu den genannten Detektionsmitteln (17, 18, 17') geschickt wird, und

dass das Mehrstationensystem eine Verschlüsselungsvorrichtung (2) zum Übertragen eines Schlüssels zu mindestens einer Sende/Empfangsvorrichtung (1) durch einen Quantenkanal (3) umfasst, wobei die Sende/Empfangsvorrichtung (1) Reflektiermittel (22) zum Reflektieren des ersten Pulses umfasst, welcher Puls durch eine Empfangsvorrichtung (1) zur genannten Empfangsvorrichtung (1) zurückgeschickt wird, und wobei die Sende/Empfangsvorrichtung (1) Reflektionsmittel (22) zum Reflektieren eines zweiten Pulses umfasst, welcher zweite Puls durch die genannte Empfangsvorrichtung (1) kurz nach dem ersten Puls zur genannten Empfangsvorrichtung (1) zurückgeschickt wird und wobei die Sende/Empfangsvorrichtung (1) Modulationsmittel (21) zum Modulieren der Phase des zweiten Pulses in Bezug auf den genannten ersten Puls umfasst.

Revendications

1. Procédé de communication entre deux postes (1, 2) utilisant un système interférométrique pour une cryptographie, comprenant l'étape d'envoi d'au moins deux impulsions lumineuses via un canal quantique (3) et de la détection de l'interférence créée par lesdites impulsions dans un poste, **caractérisé en ce que** lesdites impulsions d'interférences puissent par les mêmes ramifications dudit interféromètre mais dans une autre séquence de sorte qu'elles sont retardées lorsqu'elles sont sur ledit même canal quantique.

2. Procédé selon la revendication précédente, **caractérisé en ce que** lesdites impulsions sont réfléchies par au moins un miroir de Faraday à au moins une extrémité dudit canal quantique.

3. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** le nombre moyen de photons dans les impulsions d'interférence est inférieur à 1.

4. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** lesdites impulsions différées sont envoyées par une source (10) dans un poste émetteur/récepteur (1) qui diffère les secondes impulsions par une ligne de retour (14-16) et sont reçues par au moins un poste d'encodage (2) qui module en phase la seconde impulsion et réfléchit les deux impulsions en direction dudit poste émetteur/récepteur (1) qui diffère et qui module en phase ladite première impulsion.

5. Procédé selon la revendication précédente, **caractérisé en ce que** ladite seconde impulsion est atténuée dans ledit poste de cryptage (2) de sorte que le nombre moyen de photons dans ladite seconde impulsion réfléchie audit poste émetteur/récepteur (1) est inférieur à 1.

6. Procédé selon l'une des revendications précédentes 4 ou 5, **caractérisé en ce que** les deux postes (1, 2) sélectionnent de manière aléatoire le dé-

phasage appliqué auxdites première et seconde impulsions.

7. Procédé selon la revendication précédente, **caractérisé en ce que** lesdits déphasages sont sélectionnés soit comme valeur 0 soit comme valeur n et **en ce que** l'interférence entre ladite première impulsion et ladite seconde impulsion sont constructrices quand les deux postes ont appliqué le même déphasage et sont totalement destructrices quand ils appliquent des déphasages différents.

8. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce que** la lumière émise comprend au moins deux composants orthogonaux de polarisation et **en ce que** lesdits composants passent par les mêmes ramifications dudit interféromètre mais dans une autre séquence.

9. Procédé selon la revendication précédente, **caractérisé en ce que** l'un desdits postes (2) sélectionne au hasard la phase de l'un des composants de polarisation en tenant compte du second créant ainsi une polarisation de sortie aléatoire.

10. Système interférométrique configuré pour la distribution d'une clé par un canal quantique (3) utilisant une cryptographie quantique, comprenant :

au moins un poste émetteur/récepteur (1) et au moins un poste de cryptage, connectés tous les deux audit canal quantique (3),

des moyens (10, 12, 14, 16) dans au moins l'un desdits postes (1) pour l'envoi d'au moins deux impulsions par ledit canal quantique (3) à au moins un autre dit poste,

des détecteurs (17; 17, 18; 17') dans au moins un desdits postes (1) pour la détection de l'interférence créée par lesdits impulsions dans ledit poste,

caractérisé en ce que lesdits postes d'interférence passent par les mêmes ramifications dudit interféromètre mains dans une autre séquence de sorte qu'elles sont différées quand elles passent par ledit canal quantique.

11. Système selon la revendication précédente, **caractérisé en ce qu'**au moins l'un desdits postes (1, 2) comprend au moins un miroir de Faraday à au moins une extrémité dudit canal quantique.

12. Système selon l'une des revendications 10 ou 11, **caractérisé en ce qu'**au moins l'un desdits postes (1, 2) comprend au moins des moyens (20, 24, 12) pour atténuer l'intensité des dites impulsions lumineuses de sorte que le nombre moyen de photons dans les impulsions d'interférence est inférieur à 1.

13. Système selon l'une des revendications 10 à 12, **caractérisé en ce qu'**il comprend au moins un poste émetteur /récepteur (1) et au moins un poste encodeur (2),

ledit poste émetteur/récepteur (1) comprenant une ligne de retard (12, 14, 16) pour différer ladite première impulsion avant d'être envoyée par ledit canal quantique (3) et ladites seconde impulsion reçue par ledit canal quantique (3), et au moins un seul détecteur photon (17; 17-18; 17') pour détecter des interférences entre ladite première et seconde impulsions,

ledit poste de codage (2) comprenant des miroirs (22) pour réfléchir lesdites premières et secondes impulsions et au moins un modulateur de phase (21) pour moduler la phase d'au moins l'une desdites impulsions.

14. Système selon l'une des revendications 10 à 13, **caractérisé en ce que** ledit poste de cryptage (2) comprend des moyens (20; 24) pour atténuer l'intensité d'au moins une desdites impulsions de sorte que le nombre moyen des photons dans ladite seconde impulsion réfléchi audit poste émetteur/récepteur (1) est inférieur à 1.

15. Système selon l'une des revendications 10 à 14, **caractérisé en ce que** les deux postes (1,2) sélectionnent de manière aléatoire le déphasage appliqué aux dites première et seconde impulsions.

16. Système selon l'une des revendications 10 à 15, **caractérisé en ce que** les deux postes sélectionnent lesdits déphasages soit comme valeur 0 soit comme valeur n et **en ce que** l'interférence entre ladite première impulsion et ladite seconde impulsion sont constructrices quand les deux postes ont appliqué le même déphasage et sont totalement destructrices quand ils appliquent des déphasages différents.

17. Système selon l'une des revendications 10 à 14, **caractérisé en ce que** la lumière émise par ledit poste émetteur/récepteur (1) comprend au moins deux composants orthogonaux de polarisation et **en ce que** lesdits composants passent par les mêmes ramifications dudit interféromètre mais dans une autre séquence.

18. Système selon la revendication précédente, **caractérisé en ce que** l'un desdits postes (2) sélectionne au hasard la phase de l'un des composants de polarisation en tenant compte du second créant ainsi une polarisation de sortie aléatoire.

19. Poste de cryptage (2) pour communiquer un code clé à au moins un poste émetteur/récepteur (1) par un canal quantique (3) **caractérisé par** :

    - des moyens de réflexion (22) pour réfléchir une première impulsion renvoyée par un poste de réception (1) audit poste de réception (1),
    - des moyens de réflexion (22) pour réfléchir une seconde impulsion renvoyée par ledit poste de réception (1) juste après ladite première impulsion, audit poste récepteur (1),
    - des moyens de modulation (21) pour moduler la phase de ladite seconde impulsion par rapport à ladite première impulsion.

20. Poste de cryptage selon la revendication précédente **caractérisé par** des moyens de détection (23) pour détecter ladite première impulsion.

21. Poste de cryptage selon la revendication précédente, **caractérisé en ce que** ladite première impulsion et ladite seconde impulsion passent par lesdits moyens d'impulsion (21) et sont toutes les deux réfléchies par lesdits moyens de réflexion (22) et **en ce que** lesdits moyens de détection (23) ajutent le déphasage appliqué par lesdits moyens de modulation (21) immédiatement après avoir reçu ladite première impulsion de sorte que seulement ladite seconde impulsion est modulée en phase par lesdits moyens de modulation de phase (21).

22. Poste de cryptage selon la revendication précédente, **caractérisé en ce qu'**il sélectionne de manière aléatoire le déphasage appliqué à ladite seconde impulsion.

23. Poste de cryptage selon la revendication précédente, **caractérisé en ce que** le déphasage appliqué par ledit moyen de modulation est sélectionné de manière aléatoire soit comme valeur 0 soit comme valeur n.

24. Poste de cryptage selon l'une des revendications 19 à 23, **caractérisé en ce qu'**il comprend en outre un moyen d'atténuation (20, 24) pour atténuer l'intensité lumineuse de ladite seconde impulsion de sorte que le nombre moyen de photons dans ladite seconde impulsion réfléchie est inférieure à 1.

25. Poste de cryptage selon la revendication 24, **caractérisé en ce que** lesdits moyens d'atténuation comprennent un coupleur (20) émettant la plupart de la lumière émise auxdits moyens de détection (23).

26. Poste de cryptage selon la revendication 24 ou 25 **caractérisé en ce que** lesdits moyens d'atténuation comprend un atténuateur commandé par lesdits moyens de détection.

27. Poste de cryptage selon l'une des revendications 19 à 26, **caractérisé en ce que** lesdits moyens de réflexion (22) sont composés d'un miroir Faraday.

28. Poste de cryptage selon l'une des revendications 20 à 27, **caractérisé en ce que** lesdits moyens de réflexion ne sont pas des détecteurs de photon unique.

29. Poste de cryptage selon l'une des revendications 19 à 28, **caractérisé en ce que** lesdits moyens de modulation (21) sont faits d'un modulateur lithium Niobate ($LiNbO_3$).

30. Poste émetteur/récepteur (1) pour la réception d'une clé envoyée par un poste de cryptage (2) à travers un canal quantique (3), **caractérisé par**
    une source laser pulsée (10),
    une ligne de retard (14, 16)
    des moyens de détection (17, 18, 17"),
    un premier coupleur (12) connecté de manière que les impulsions émises par ladite source laser pulsée soient divisées en deux impulsions, la première dite impulsion divisée est envoyée directement audit canal quantique tandis que la seconde impulsion divisée est différée par ladite ligne de retard (14, 16) avant d'être envoyée audit canal quantique et en ce que les impulsions reçues par ledit canal quantique (3) sont divisées en deux impulsions, la première impulsion étant envoyée directement auxdits moyens de détection (17, 18, 17') tandis que la seconde impulsion est différée par ladite ligne de retard (14, 16) avant d'être envoyée auxdits moyens de détection (17, 18, 17").

31. Poste émetteur/récepteur selon la revendication précédente **caractérisé par** des moyens de modulation (13) pour moduler la phase des impulsions reçues différées par ladite ligne de retard (14, 16).

32. Poste émetteur/récepteur selon la revendication précédente **caractérisé en ce que** lesdits moyens de modulation (13) sélectionnent au hasard le déphasage appliqué auxdits impulsions différées.

33. Poste émetteur/récepteur selon la revendication précédente **caractérisé en ce que** lesdits moyens de modulation (13) sélectionnent au hasard le déphasage soit comme valeur 0 soit comme valeur n.

34. Poste émetteur/récepteur selon l'une des revendications 31 à 33, **caractérisé en ce que** les moyens de modulation (21) sont faits d'un modulateur lithium Niobate ($LiNbO_3$).

35. Poste émetteur/récepteur selon la revendication 30, **caractérisé en ce qu'**il comprend deux détecteurs (17, 18), **en ce que** ledit premier coupleur (12') est un coupleur 3x3 connecté auxdits détecteurs (17, 18) et **en ce qu'**une impulsion va être envoyée soit sur le premier (17) soit sur le second (18) desdits détecteurs dépendant de l'interférence créée dans ledit coupleur (12').

36. Poste émetteur/récepteur selon la revendication 30 **caractérisé en ce que** ladite source laser (10) envoie des impulsions lumineuses avec une polarisation circulaire et **en ce que** ledit premier coupleur (12") est un coupleur de polarisation qui sépare les polarisations verticales et horizontales des pulsions.

37. Poste émetteur/récepteur selon la revendication 30, **caractérisé en ce que** ladite ligne de retard (14, 16) comprend deux miroirs Faraday (14, 16) réfléchissant les impulsions différées.

38. Poste émetteur/récepteur selon l'un des revendications 30 à 37, **caractérisé en ce que** lesdits moyens de détection (17, 18, 17') sont des détecteurs de photon unique.

39. Poste émetteur/récepteur selon la revendication précédente **caractérisé en ce que** lesdits détecteurs de photon unique (17, 18, 17') sont des photodiodes à avalanche au-delà du claquage inverse et fonctionnant en mode Geiger.

40. Poste émetteur/récepteur selon l'un des revendications 38 ou 39, **caractérisé en ce que** pour réduire le nombre de Dark Count, les détecteurs de photon unique ne sont activés qu'à chaque fois qu'un photon est attendu.

41. Poste émetteur/récepteur selon l'un des revendications 30 à 40, **caractérisé en ce que** ladite source laser pulsée est un laser DFB.

42. Poste émetteur/récepteur selon l'un des revendications 30 à 41, comprenant en outre des moyens de correction d'erreur.

43. Dispositif pour la distribution d'une clé par un canal quantique (3) utilisant une cryptographie quantique, **caractérisé en ce qu'**il comprend un poste émetteur/récepteur (1) pour recevoir une clé émise par un poste de cryptage (2) via un canal quantique (3), le poste émetteur/récepteur (1) comprenant une source laser pulsée (10) une ligne de retard (14, 16), des moyens de détection (17, 18, 17') et un premier coupleur (12) connecté de manière que les impulsions émises par ladite source laser pulsée soient divisées en deux impulsions, la première impulsion divisée étant envoyée directement audit canal quantique, tandis que la seconde impulsion divisée est différée par ladite ligne de retard (14, 16) avant d'être envoyée par ledit canal quantique et **en ce que** les impulsions reçues dudit canal quantique (3) sont divisées en deux impulsions, la première impulsion étant envoyée directement audit moyens de détection (17, 18, 17') tandis que la seconde impulsion est différée par ladite ligne de retard (14, 16) avant d'être envoyée auxdits moyens de détection (17, 18, 17'), et

en ce qu'il comprend une poste de cryptage (2) pour communiquer une clé à au moins un poste émetteur/récepteur (1) par un canal quantique (3), tandis que le poste émetteur/récepteur (1) comprend des moyens de réflexion (22) pour réfléchir une première impulsion par un poste récepteur (1) audit poste récepteur (1), des moyens de réflexion (22) pour réfléchir une seconde impulsion envoyée par ledit poste récepteur (1) juste après la dite première impulsion audit poste récepteur (1) et des moyens de modulation (21) pour moduler la phase de ladite seconde impulsion par rapport à ladite première impulsion.

44. Système multiposte par la distribution d'une clé par un canal quantique (3) utilisant une cryptographie quantique entre au moins un poste émetteur/récepteur (1) et au moins un poste de cryptage (2) **caractérisé en ce**

qu'il comprend un poste émetteur/récepteur (1) pour recevoir une clé émise par un poste de cryptage (2) via un canal quantique (3), le poste émetteur/récepteur (1) comprenant une source laser pulsée (10), une ligne de retard (14, 16), des moyens de détection (17, 18, 17') et un premier coupleur (12) connecté de manière que les impulsions émises par ladite source laser pulsée soient divisées en deux impulsions, la première impulsion divisée étant envoyée directement audit canal quantique, tandis que la seconde impulsion divisée est différée par ladite ligne de retard (14, 16) avant d'être envoyée par ledit canal quantique et en ce que les impulsions reçues dudit canal quantique (3) sont divisées en deux impulsions, la première impulsion étant envoyée directement auxdits moyens de détection (17, 18, 17') tandis que la seconde impulsion est différée par ladite ligne de retard (14, 16) avant d'être envoyée auxdits moyens de détection (17, 18, 17'), et

en ce qu'il comprend une poste de cryptage (2) pour communiquer une clé à au moins un poste émetteur/récepteur (1) par un canal quantique (3), tandis que le poste émetteur/récepteur (1) comprend des moyens de réflexion (22) pour réfléchir une première impulsion par un poste récepteur (1) audit poste récepteur (1), des moyens de réflexion (22) pour réfléchir une seconde impulsion envoyée

par ledit poste récepteur (1) juste après la dite première impulsion audit poste récepteur (1) et des moyens de modulation (21) pour moduler la phase de ladite seconde impulsion par rapport à ladite première impulsion.

FIG. 1

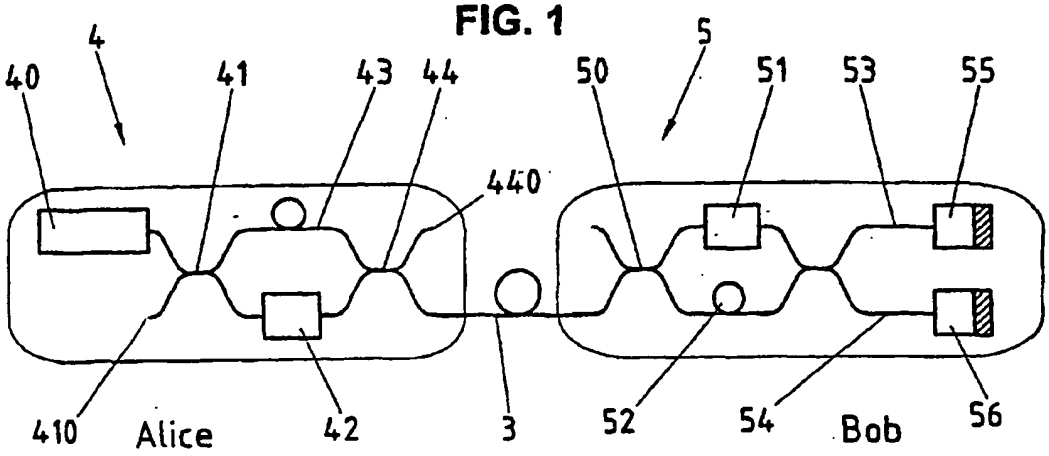

4
5
40
41
43
44
50
51
53
55
440
410
Alice
42
3
52
54
Bob
56

FIG. 2

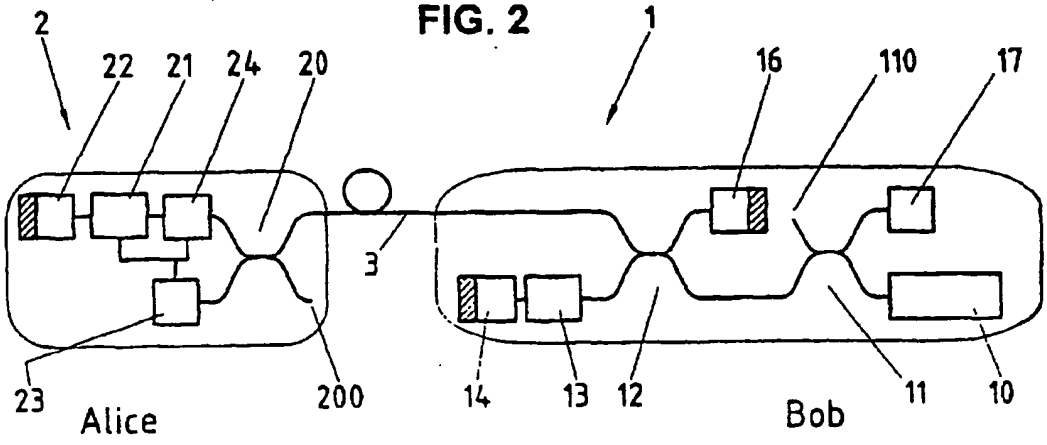

2
1
22
21
24
20
16
110
17
3
23
Alice
200
14
13
12
Bob
11
10

FIG. 3

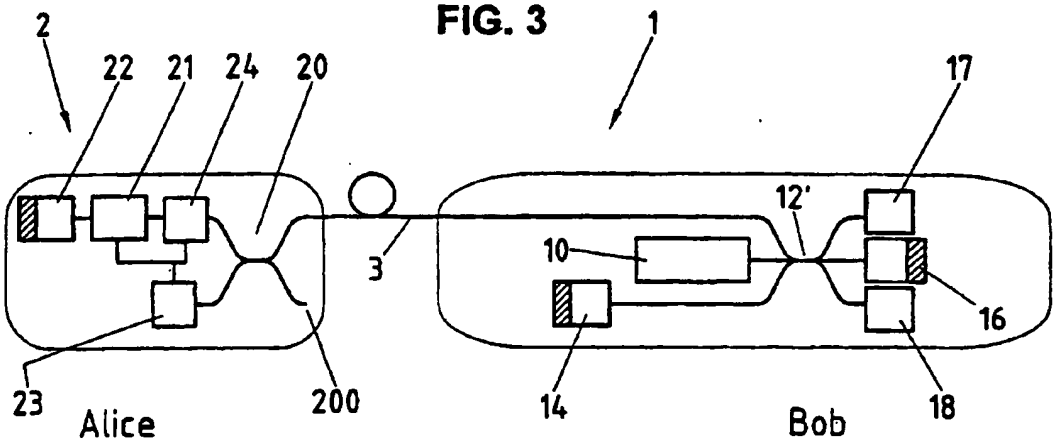
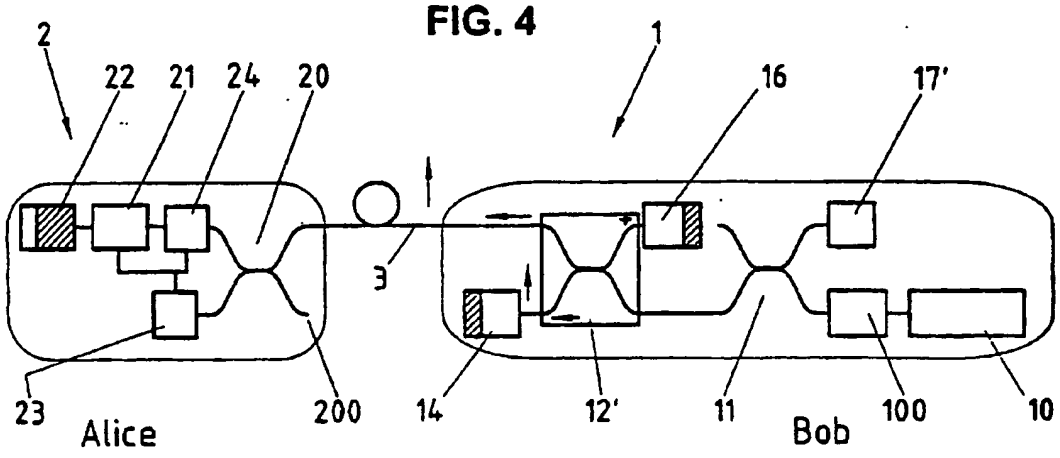

2
22
21
24
20
1
17
12'
10
3
16
23
200
14
18
Alice
Bob

FIG. 4


2
22
21
24
20
1
16
17'
3
23
200
14
12'
11
100
10
Alice
Bob